

March 2008

DEFENSE ACQUISITIONS

Significant Challenges Ahead in Developing and Demonstrating Future Combat System's Network and Software



G A O

Accountability * Integrity * Reliability

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE MAR 2008		2. REPORT TYPE		3. DATES COVERED 00-00-2008 to 00-00-2008	
4. TITLE AND SUBTITLE Defense Acquisitions: Significant Challenges Ahead in Developping and Demonstrating Future Combat System's Network and Software				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Government Accountability Office ,441 G St NW,Washington,DC,20548				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 43	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			



Highlights of [GAO-08-409](#), a report to Congressional Committees

Why GAO Did This Study

The Army's Future Combat System (FCS) requires a software-based advanced information network to meld people, sensors, and weapons into a cohesive fighting force. As software controls 95 percent of FCS's functionality, it determines the success or failure of the program. The Army contracted with the Boeing Company as a lead systems integrator (LSI) to define, develop and integrate FCS, including software development.

GAO must by law report annually on FCS. This is one of two reports to meet this requirement. It addresses risks facing the development of network and software, the practices being used to manage software, and the timing of key network demonstrations.

In conducting our work, GAO has contacted numerous DOD, Army, and contractor offices; reviewed technical documents on software and network development and plans; attended meetings; and spoken to Army and other officials on various aspects of FCS network and software development. GAO also performed detailed work at five FCS software developers.

What GAO Recommends

GAO recommends that the Secretary of Defense direct the program to stabilize network and software requirements on each build to enable adherence to disciplined practices and establish clear criteria on acceptable network performance and demonstrations at each of the key program events. DOD concurred with GAO's recommendations.

To view the full product, including the scope and methodology, click on [GAO-08-409](#). For more information, contact Paul L. Francis at (202) 512-4841 or francisp@gao.gov.

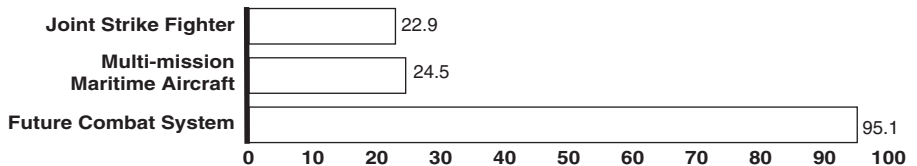
DEFENSE ACQUISITIONS

Significant Challenges Ahead in Developing and Demonstrating Future Combat System's Network and Software

What GAO Found

Almost 5 years into the program, it is not yet clear if or when the information network that is at the heart of the FCS concept can be developed, built, and demonstrated by the Army and LSI. Significant management and technical challenges have placed development of the network and software at risk. These risks include, among others, network performance and scalability, immature network architecture, and synchronization of FCS with Joint Tactical Radio System and Warfighter Information Network Tactical programs that have significant technical challenges of their own. Software being developed for the network and platforms is projected to total 95.1 million lines of computer code, almost triple the size since the program began in 2003. As shown, FCS's software is about four times larger than the next two largest software-intensive defense programs.

Comparison of FCS Software Size to the Next Largest Software Intensive Defense Programs
Source lines of code (in millions)



Source: Army, Navy, Air Force (data); GAO (analysis and presentation).

Although several disciplined practices are being used to develop FCS's network and software, the program's immaturity and aggressive pace during development have delayed requirements development at the software developer level. For example, software developers for 5 major software packages that GAO reviewed report that high-level requirements provided to them were poorly defined, late, or omitted in the development process. This caused the software developers to do rework or defer functionality out to future builds. In turn, these poor or late requirements had a cascading effect that caused other software development efforts to be delayed.

It is unclear when or how it can be demonstrated that the FCS network will work as needed, especially at key program junctures. For example, in 2009, network requirements, including software, may not be adequately defined nor designs completed at the preliminary design review; and at the FCS milestone review later that year, network demonstration is expected to be very limited. The first major FCS network demonstration—the limited user test in 2012—will take place at least a year after the critical design review and only a year before the start of FCS production. That test will seek to identify the impact of the contributions and limitations of the network on the ability to conduct missions. This test will be conducted after the designs have been set for the FCS ground vehicles, which poses risks because the designs depend on the network's performance. A full demonstration of the network with all of its software components will not be demonstrated until at least 2013 when the fully automated battle command system is expected to be ready.

Contents

Letter		1
	Results in Brief	2
	Background	4
	Unclear If or When the Army Can Develop, Build, and Demonstrate the FCS Network	10
	Software Practices Have Been Adopted, but Implementation Has Been Hampered by Evolving Requirements	18
	Uncertainty about Network Development and Demonstration Present Challenges for Decisionmakers at Key Program Events	23
	Conclusions	26
	Recommendations for Executive Action	27
	Agency Comments and Our Evaluation	27
Appendix I	Scope and Methodology	31
Appendix II	Comments from the Department of Defense	32
Appendix III	List of FCS Software (Network & Non-network) Packages Developed by Contractors (as of July 2007)	35
Appendix IV	GAO Contact and Staff Acknowledgments	36
Related GAO Products		37
Tables		
	Table 1: FCS Software Growth Estimates	15
	Table 2: Software Packages and Associated Requirements Problems	22
Figures		
	Figure 1: Examples of Sensors for FCS Brigade Combat Teams	7

Figure 2: Visual Depiction of How the Warfighter Could See the Battlefield	8
Figure 3: JTRS Radios for FCS Platforms	10
Figure 4: Comparison of FCS Software SLOC Size to Other Major Defense Programs	17
Figure 5: Traditional Spiral Development Illustration	19
Figure 6: FCS Spiral Development Strategy and Software Life Cycle Reviews	23

Abbreviations

BCT	Brigade Combat Team
DOD	Department of Defense
FCS	Future Combat System
JTRS	Joint Tactical Radio System
LSI	lead systems integrator
SOSCOE	System of Systems Common Operating Environment
WIN-T	Warfighter Information Network-Tactical

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

March 7, 2008

Congressional Committees

The Army's transformation to a lighter, more agile, better equipped, and more lethal and survivable combat force—the Future Combat System (FCS) program, which comprises 14 integrated weapon systems—depends on successfully developing an advanced information network that links people, platforms, weapons, and sensors together. The FCS program is considered by the Army to be the greatest technology and integration challenge that they have ever undertaken and the network may be the most important element of FCS. In order to make this leap, software and technology must be developed that will allow the network to (1) collect, process, and deliver vast amounts of information such as imagery and communications; (2) seamlessly link people and systems; and (3) integrate and enhance the individual performance of the systems themselves. Because software is expected to control about 95 percent of FCS's functionality, it is the linchpin to the success or failure of the program. The magnitude, size, and complexity of the network and software development are unprecedented in the Department of Defense's (DOD) history. To help them with this ambitious endeavor, the Army contracted with the Boeing Company as the lead systems integrator (LSI) in 2003 to define, develop, and integrate FCS, including software development that is being done in cooperation with the FCS program office.

Given its cost, scope, and technical challenges, section 211 of the National Defense Authorization Act for Fiscal Year 2006 requires GAO to report annually on the FCS program.¹ As one of two reviews conducted this year by GAO under this authority, this report addresses (1) challenges and technological risks that could hamper successful development of the network and software, (2) whether disciplined software practices have been effectively implemented for managing development of FCS's network and software, and (3) whether the Army will have the necessary network and software at key program events such as preliminary design review, critical design review, and start of FCS production. A second report

¹ Pub. L. No. 109-163, § 211 (2006).

addresses the specific elements of section 211 to include FCS development, production, and cost issues.²

In conducting our work, we have contacted numerous DOD, Army, and contractor offices. We also conducted detailed work and held discussions with selected contractors on their efforts to develop five major software packages that are to operate the network, training, combat identification, and other elements for FCS. We reviewed technical network and software plans, assessments, and studies pertaining to the FCS program, attended meetings at which DOD and Army officials reviewed program progress, and held discussions with key Army and LSI officials on various aspects of the network and software development for FCS. Officials from DOD, Army, and LSI have provided us access to sufficient information to make informed judgments on the matters in this report. In addition, we drew from our body of past work on weapon systems acquisitions practices and software development best practices. We conducted this performance audit from July 2007 to March 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Appendix I further discusses our scope and methodology.

Results in Brief

It is not yet clear if or when the Army and LSI can develop, build, and demonstrate the information network that is at the heart of the FCS concept. The Army is faced with significant management and technological challenges that place development of FCS's network and software at risk. Almost 5 years into the program, the Army and LSI have not yet fully defined how the FCS network is expected to function, how they plan to build it, and how they plan to demonstrate it. The Army and LSI have identified and need to address numerous areas of high risk such as network performance and scalability, immature network architecture, and synchronization of FCS with the Joint Tactical Radio System (JTRS) and Warfighter Information Network Tactical (WIN-T) programs, which are having difficulty with technology maturation and are at risk of being delayed or delivering incomplete capabilities to FCS. Software being

² GAO, *Defense Acquisitions: 2009 Is a Critical Juncture for the Army's Future Combat System*. [GAO-08-408](#) (Washington, D.C.: Mar. 7, 2008).

developed for the network and platforms by the LSI and software developers is now projected to total about 95.1 million lines of computer code, which almost triples the size since the program began in 2003. A June 2006 report issued by the Secretary of Defense's Cost Analysis Improvement Group found that the FCS program is at risk of higher costs due to, among other things, the size and complexity of the FCS software development program. This group also said the development schedule is highly likely to take several years beyond the Army's plan, and the network is at risk because it is tied to JTRS and WIN-T programs that could cause delays in FCS's development schedule. Similarly, a recent study by the Institute for Defense Analysis found that the FCS program would likely experience additional growth in unplanned software effort, unplanned rework before and after operational testing, and additional work to address system of systems integration, validation, and test after the critical design review point.

While the Army and LSI have implemented several disciplined practices that have proven successful at leading software companies, such as the use of repeatable and managed development processes and use of a structured management review process to ensure quality development, we found that the immature definition of system-level requirements by the Army and LSI was causing problems. For example, the software developers for the five major software packages we reviewed report that high-level requirements provided to them by the LSI for decomposition and refinement were poorly defined, omitted, or late in the software development process. Also, we found that poor or late requirements development has had a cascading effect as late delivery or poorly defined requirements on one software development effort, in turn, caused other software development efforts to be delayed. For example, four of the five software developers report that problems with late requirements have caused them to do rework or to defer functionality out to future builds because of insufficient time. These software developers report that schedule compression caused much of this strain, which could have been averted if they had been allowed sufficient time to adequately understand and analyze the requirements.

It is unclear when or how the Army and LSI will be able to demonstrate that the network will work as needed, which poses risks for the designs of individual FCS systems and the ability to assess FCS's viability at key decision points. For example, it is unclear if network requirements, including software to be developed, will be adequately defined and designs completed at the preliminary design review scheduled for February 2009. To date, only some elementary aspects of the FCS network, such as basic

connectivity have been demonstrated. At the time of the FCS milestone review in 2009, the extent of network demonstration is expected to be very limited. For example, the Army expects to demonstrate some network functions, such as linkage with remote sensors, during the spinout demonstrations in fiscal year 2008. Other limited demonstrations are scheduled on a regular basis. However, the first major demonstration of the FCS network is the limited user test scheduled for fiscal year 2012, which will be at least a year after the critical design review and only about a year before the start of FCS production. This event comes after the vehicle designs on manned ground platforms have been established. One of the key objectives of that test will be to identify the contributions and limitations of the network regarding the ability of the FCS brigade combat team to conduct missions across the full spectrum of operations. However, the fully automated battle command system is not expected until 2013 when the Army expects 100 percent of the network capabilities including software to be available.

We are making recommendations to the Secretary of Defense regarding the stabilization of network and software requirements on each build to enable adherence to disciplined software practices, and establishment of clear performance criteria for acceptable network performance and demonstrations at each of the key program events. In commenting on a draft of this report, DOD concurred with our recommendations.

Background

The advanced information network is the heart of the Army's FCS concept and is intended to allow fielded FCS Brigade Combat Teams (BCT) to see the enemy first, understand the situation first, act first, and finish decisively. The FCS network management system to be deployed to the Army's BCT is envisioned to: (1) plan and manage multi-technology mobile tactical communication; (2) encompass satellite, aerial and ground communication assets that provide multi-media voice, data, and video services to all elements of the FCS BCT; and (3) interface with terrestrial, aerial, and satellite assets of an Army division. If the FCS network works as intended, all commanders in the BCT and throughout areas of operations will have a common set of data that will allow for the synchronization of many BCT activities including the integration of fire and maneuver, intelligence collection, fusion, and dissemination, and sustainment of the force. The Army envisions that the network architecture would also permit connectivity with other military services, thus allowing additional situational awareness and understanding, and synchronized operations that are unachievable by current systems.

FCS-equipped BCTs are to have significant warfighting capabilities that differ substantially from the large division-centric structure. The survival and combat effectiveness of FCS BCTs are critically dependent on the ability to see first, understand first, act first, and finish decisively. Through an advanced information network, the concept is to replace mass with superior information that will allow soldiers to see and hit the enemy first rather than to rely on heavy armor to withstand a hit. This new way of fighting solely depends on developing an information network that can successfully link the people, platforms, weapons, and sensors seamlessly together in a system of systems. This new way of fighting can be achieved only if the data can be made available in near real-time at sensor processors, at the battle command nodes, and at lethal systems. For example, FCS's survivability depends on the brigade-wide availability of the network-based situational awareness plus the inherent survivability of the FCS platforms.

FCS Network Elements

Elements of the FCS information network will include the software and technology (applications, computers, and radios) that will link the people, platforms, weapons, and sensors together. These elements are expected to provide delivery of voice, data, video, still images, and network control services wirelessly over a mobile ad hoc network.³ In contrast to traditional wireless systems such as cellular phones that connect to a fixed station or permanent access point, FCS's ad hoc network will not have access to such an infrastructure. Thus, the quality of service—the capability to transport information across the network while satisfying communication performance requirements such as low delay, low loss, or high throughput—becomes critically important and challenging due to limited available bandwidth.⁴ Essentially, tasks like mission planning,

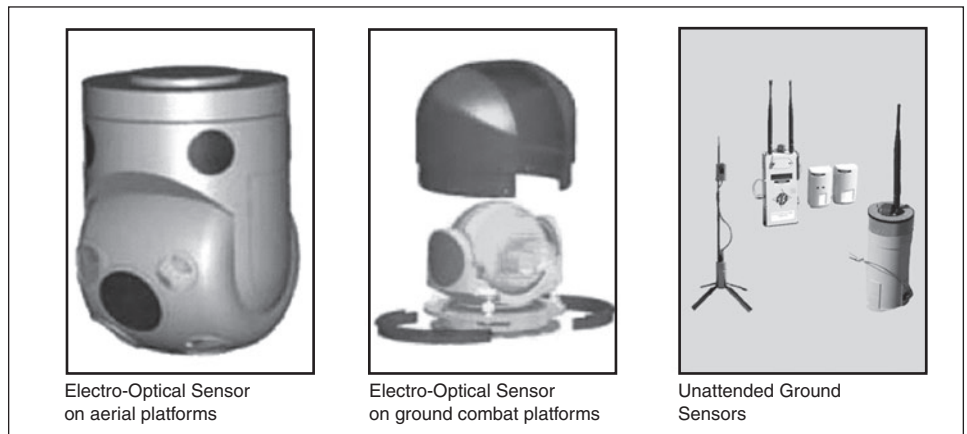
³ A mobile ad-hoc network is an autonomous collection of mobile users that communicate over relatively bandwidth-constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, meaning all network activity including discovering the topology and delivering messages must be executed by the nodes themselves (i.e., routing functions will be incorporated into mobile nodes). In a military environment such as FCS, ensuring security and reliability are major concerns. Military networks are designed to maintain a low probability of intercept and/or a low probability of detection. Hence, nodes are to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection or interception. A lapse in any of these requirements may degrade the performance and dependability of the network.

⁴ Bandwidth is a term used in much of the telecommunications industry as a measure, usually expressed in bits per second, of the rate at which information moves from one electronic device to another.

platform and soldier logistics management, battlespace analysis, collaboration, fire and effect controls, and network management will be done on the move. All of the 14 FCS platform types—manned ground vehicles, unmanned ground vehicles, unmanned air vehicles, and unattended ground sensors—are expected to have network elements that will enable them to share information and coordinate with one another. These elements include:

Sensors. Sensors are the hardware and software that will provide FCS with the ability to “see first” and achieve situational awareness and understanding of the battlefield. These sensors will include such functions as search and detection of enemy fire, personnel, munitions, minefields, and terrain. The intelligence, surveillance and reconnaissance sensors will be integrated onto all manned and unmanned ground vehicles and aerial platforms, and will be capable of accomplishing a variety of missions that include, among others, surveillance over wide areas and target detection, enabling survivability. The unmanned aerial vehicles will be able to maneuver to an area of attack and the on-board sensors will provide surveillance of targets and terrain, among other functions. There are two types of unattended ground sensor systems that FCS will use—the tactical unattended ground sensors will provide intelligence, surveillance, and reconnaissance awareness to the BCTs, while urban unattended ground sensors will support clearing operations in confined spaces or urban chokepoints. According to the Army, complex data processing, filtering, aided target recognition, and fusion will be supported by software to provide warfighters with vital information. For example, the sensor data management software will organize the sensor data and track the information received from sensors. Figure 1 shows some types of FCS sensors.

Figure 1: Examples of Sensors for FCS Brigade Combat Teams



Source: U.S. Army.

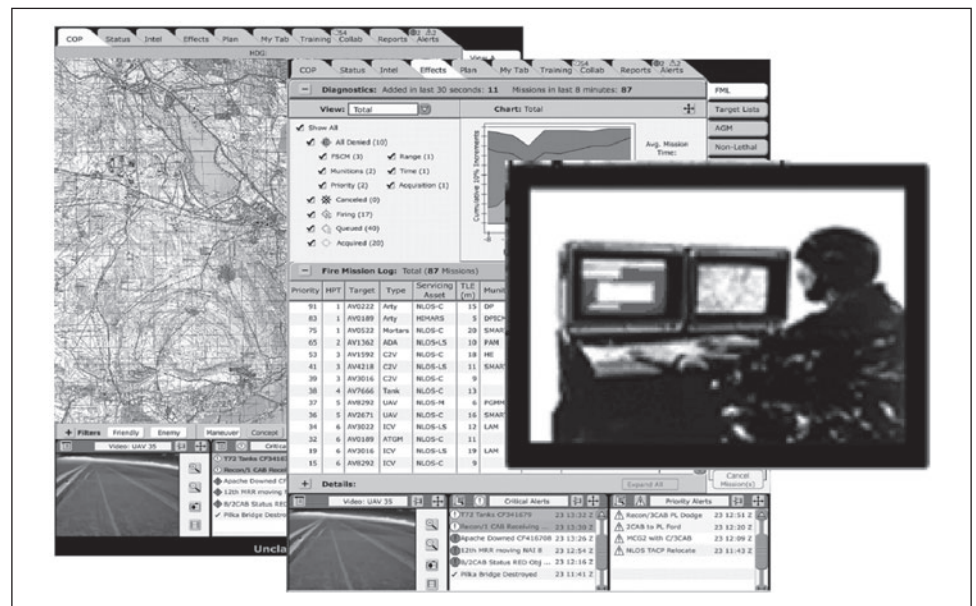
Software. Software is expected to control about 95 percent of FCS's functionality and will be included in all FCS platforms. In its simplest form, software is the collection of computer programs and procedures that perform some task on a computer system or platform. It includes: (1) system software such as operating systems, which interface with hardware to provide the necessary services for application software; (2) middleware, which controls and coordinates distributed systems; and (3) application software such as word processors, which perform productive tasks for users. Overall development of FCS software is being managed by the LSI in cooperation with the Army's FCS Program Office. There are over 100 software vendors involved in the development of software programs for FCS, including the LSI, 14 first-tier contractors, and other sub-contractors.

Over 75 percent of software being developed for FCS is to operate the network. Network software is expected to integrate the collection of individual systems into a system of systems. This software will include the System of Systems Common Operating Environment (SOSCOE), Network Management System, Battle Command and Mission Execution, Sensor Data Management, Warfighter Machine Interface⁵, and others. These will be included on all the FCS platforms and will perform a variety of functions. For example, software on platforms is to control the

⁵ The Warfighter Machine Interface software is to be part of manned systems and warfighter or soldier systems only.

individual systems, such as radios and air and ground vehicle communications. SOSCOE is the operating environment that serves as the middleware between the operating systems and the software applications, integrating all other FCS software. The Battle Command software is to provide functions such as mission planning and preparation, situational understanding, and battle management and mission execution. Warfighter Machine Interface software is expected to provide the visual interface of the network to the warfighter. According to the Army, Warfighter Machine Interface is “the face of the FCS network,” which includes the display of services, touch screens, and buttons. It will provide a visual picture of the battlespace and allows the ability to collaborate across the forces. Figure 2 shows how the warfighter may see the battlefield through the network.

Figure 2: Visual Depiction of How the Warfighter Could See the Battlefield



Source: U.S. Army.

Integrated Computing System. The integrated computing system is the on-board computer that will fit into the various FCS platforms. There are eight types of Integrated Computing Systems that vary in size to fit into the various FCS platforms—manned ground vehicles, unmanned aerial vehicles, and unattended ground vehicles. The computing system is expected to provide an integrated common operating environment to manage processing, secure the system, and allow access to the network

on the move. It is also envisioned to support battle command applications, sensor processing, communications, weapons and platform management, and have embedded security and safety features that will help ensure a secure operating environment with certified firewall and network intrusion protection.

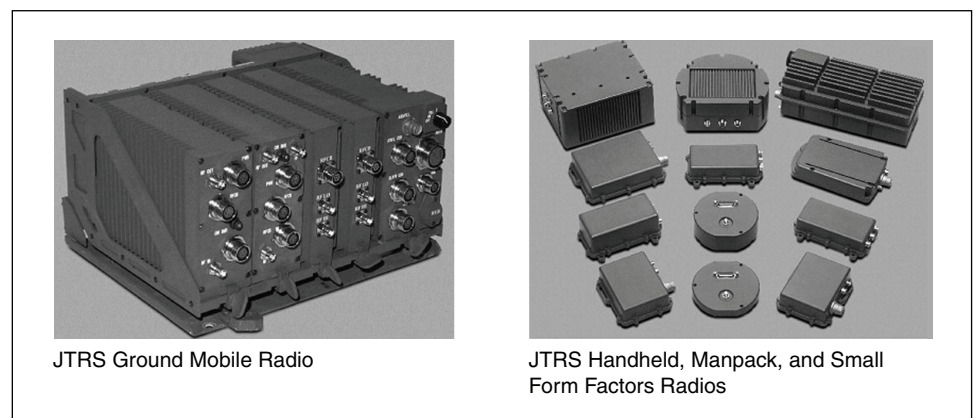
Joint Tactical Radio System (JTRS)/Warfighter Information Network-Tactical (WIN-T). The Army plans to use the JTRS and WIN-T radios that employ “software-defined radio” technology in which many functions are performed by computer processing and technology. These and other critical software-intensive technologies are being developed outside of FCS control—termed complementary programs—and are expected to interoperate with existing systems and provide additional communications capability. The JTRS family of software-based radios is to provide the high-capacity, high-speed information link to vehicles, weapons, aircraft, sensors, and soldiers, while WIN-T is to provide high bandwidth connectivity to Army units on the move with higher levels of command to other forces, and provide the Army’s tactical extension to the Global Information Grid.⁶ Such capabilities include access to maps and other visual data, communication via voice and video with other units and levels of command, and the acquisition of information directly from battlefield sensors. The JTRS family of programs includes the Ground Mobile Radios that are being developed for vehicles. Smaller JTRS Handheld, Manpack, and Small Form Factors radios are being developed that will be carried by soldiers and embedded in several FCS core systems. Software will be used to control how JTRS radios will work. For example, JTRS radios will use two software waveforms⁷ called the Wideband Networking Waveform and Soldier Radio Waveform. The function of the Wideband Networking Waveform software is to provide

⁶ The Global Information Grid is a large and complex set of programs and initiatives intended to provide Internet-like capability allowing users at virtually any location to access data on demand, share information in real time, and collaborate in decision making, regardless of which military service produced which weapon system, thus having greater joint command of a battle situation.

⁷ A waveform is the representation of a signal that includes the frequency, modulation type, message format, and/or transmission system. In general usage, the term waveform refers to a known set of characteristics, for example, frequency bands (VHF, HF, and UHF), modulation techniques (FM, AM), message standards, and transmission systems. In JTRS usage, the term waveform is used to describe the entire set of radio functions that occur from the user input to the RF output and vice versa. A JTRS waveform is implemented as a reusable, portable, executable software application that is independent of the JTRS operating system, middleware, and hardware.

communications signals, routing, transport, network management, quality of service, information assurance, transport, and mobility. The Soldier Radio Waveform is being developed for JTRS radios—ground mobile radio, and handheld manpack and small form factors radios—and will primarily be used for tactical networking by soldiers, unattended systems, and embedded radios in munitions. Because FCS has unique applications and networking needs, the program is responsible for integrating these into their distributed applications that are running on SOSCOE. Figure 3 shows the JTRS radios.

Figure 3: JTRS Radios for FCS Platforms



Source: U.S. Army.

Unclear If or When the Army Can Develop, Build, and Demonstrate the FCS Network

The Army is faced with significant management and technological challenges that place development of the FCS network at risk. All of the projected FCS capabilities are heavily dependent on wide availability and high performance of the network. Further, preliminary design of the network is still being matured and much development and integration of the network hardware and software remains. It has taken almost 5 years for the Army and LSI to develop an understanding of what the network needs to be, what may be technically feasible, how to build it, and how to demonstrate it. In addition, the definition of the detailed network requirements is still not complete and there are numerous risks that must be overcome, such as the constraints imposed by a mobile ad hoc network, gaps between FCS network design and complementary program requirements, and interoperability issues with strategic networks of the Global Information Grid. While progress has been reported on software development, the continued growth in software code and underestimation

of what it will take to develop and integrate software poses risk to the successful development of the network.

Army Has Reached Understanding of the Network

Although maturity of network design is still a work in progress (i.e., numerous high risks remain and full network demonstration is years away), the Army has achieved an understanding of what the network needs to be, what may be technically feasible, how to build it, and how to demonstrate it. However, in addition to challenges and risks that need to be addressed, much learning and work remains before the Army and LSI can mature the network. For example, the Army and LSI are still determining what network management means in terms of: (1) what is needed to support each specific mission (radios, routers, satellites, computers, information assurance devices, and policies); (2) how to allocate network resources to the mission spectrum; and (3) how to fuse, process, and present extensive FCS sensor data to appropriate users. They are also learning how to maintain the network, such as monitoring the status and performance of the network (hardware faults, network quality of service, and overall performance); managing the spectrum to ensure connectivity; avoiding interference; and reconfiguring the network in real-time based on changing network conditions and mission critical traffic.

To provide managed communication services between the soldiers, platforms, and sensors to complete military missions successfully, the Army must decide what information the individual users will need and its priority, where that information may reside, and how and when to get it to the user. For example, current plans call for the network supporting a BCT to include more than 5,000 nodes on over 1,500 radio sets running at least four different advanced networking waveforms, supporting networks and sub-networks interconnected by gateways, and carrying 3 million identified, point-to-point information exchange requirements.⁸ The Army's FCS program office provides that the primary interface types for FCS will include discovery, publish/subscribe, and multi-cast methods. Given the reality that the amount of traffic to be sent over the network may exceed its capacity, assuring end-to-end quality of service over the network presents a major challenge. The Army and LSI have undertaken studies to better understand it.

⁸ FCS Program Office, "Network Quality of Service Analysis (SDD-129): System of Systems Engineering and Integration, Document Number: D786-11421-1, July 28, 2005.

Mobile Adhoc Networks Have Inherent Constraints

The Army and LSI are in the midst of developing the next generation of wireless communications, referred to as the mobile ad hoc network, which is a fundamentally new capability that presents a host of technical challenges. For example, the mobile ad hoc network will operate with lower network capacity and have fewer options for increasing capacity due to limitations on the amount of radio frequency that is available. Performance of the ad hoc network is expected to decrease as more radios or nodes are added and eventually can reach an unacceptable level. That is, the size of the network may reach a maximum when all fixed capacity is consumed for routing traffic from other radios or nodes and no capacity is available for local consumption. In a network of limited capacity, decisions need to be made on how to control admission to the network, account for network resources, ensure end-to-end services basis, and do so in a mobile ad hoc network environment with varying routes and link capacities. As a result, the Army and LSI are working on how best to allocate functions throughout the FCS system of systems.

Further, unlike common wireless systems that have access to the Internet—such as cellular and wireless networking protocols where every node is connected directly to the network by a single local wireless link—the FCS information network will change dynamically as the mobile nodes are expected to be able to communicate with each other, while on the move. In the FCS information network, most network nodes will not have local access to the network. Thus, each radio must also be a router, meaning that it is responsible for passing traffic (voice, data, and video) from other radios as well as traffic local to the radio. As a result, networking becomes extremely difficult for the following reasons:

- The FCS information network is wireless and, consequently, the bandwidth limits the availability of the radio frequency spectrum.
- A mobile ad hoc network has known characteristics that pose difficulties in providing quality of service such as, among others, the lack of precise information about network performance, lack of central control, and insecure media over the network.

The research community is still studying various approaches and trade-offs to these open problems because they are not yet fully understood. Because these problems have not been solved and are not supported by an existing and proven technology base, there is serious concern whether the Army and LSI can overcome them within the current schedule.

Network Risks Identified

While some progress is being made to understand what the network needs to be, how to build it, and how to demonstrate it, the Army and LSI have identified major technical and integration risks to be addressed in order to meet overall FCS requirements. In July 2007, the Army and LSI reported their findings from a network review that identified 7 high-risks and 16 medium-risks, totaling 23 risks specific to the FCS network. Although Army and LSI officials are confident that such risks can be addressed, the scale and complexity of what is involved is without precedent. Among others, network risks include:

- Enterprise network performance and scalability. There is a high likelihood that the FCS network performance will be affected because ad hoc networks have limited scalability, and performance decreases as more radios are added.
- End-to-end quality of service on mobile ad hoc networks. The probability is high that the FCS network will not be able to ensure that the information with the highest value is delivered on time to the intended recipients. Failure to support the warfighter in defining and implementing command intent for information management will result in substantially reduced force effectiveness. These capabilities are dependent on actual performance of JTRS and WIN-T, both of which have their own technology, development, and programmatic difficulties and are at risk of being delayed or delivering incomplete capabilities. The FCS Program Office and LSI are working closely with program offices responsible for managing these complementary programs, but synchronization of the detailed requirements is still problematic.
- End-to-end interoperability with strategic networks of the Global Information Grid. The requirements of interoperability with strategic networks of the Grid will be another challenge. Given the already stressed conditions envisioned for FCS tactical networks, interoperability with strategic networks will be technically challenging.
- Soldier radio waveform availability. The soldier radio waveform provides functional capability that is needed to support many FCS systems but may not be completed in time to support FCS. These capabilities facilitate interoperability functions between the FCS family of systems. The development of waveforms remains a technically challenging and lengthy effort, which involves complex software development and integration work. The program has already experienced schedule delays, cost increases, and requirements changes. As such, these functional capabilities are critical to FCS's performance and these delays will negatively impact the schedule.

-
- System of Systems Common Operating Environment availability and maturity. There is recognized risk that SOSCOE may not reach the necessary maturity level required to meet program milestones. There are also recognized risks associated with interoperability of the software and dissemination of data to the mobile ad hoc network.
 - Software productivity. There is recognized high risk that the LSI and its contractors may not be able to build, test, and integrate as much software as planned in the projected times. If software productivity falls short of planned efforts, the overall software build schedules will be impacted by 2 to 4 months, and integration will also be correspondingly impacted.

Software Code Estimates Continue to Grow

The amount of estimated software code required for FCS has recently increased to 95.1 million lines. This is nearly triple the original estimate made in 2003 and the largest software effort by far for any weapon system. Software code is difficult to estimate and underestimation is not unique to FCS. Compounding this inherent difficulty on FCS were the program's poorly defined requirements, indicative of its immaturity. Lines of code have grown as requirements have become better understood. While the Army believes the latest increases will not command higher costs, independent estimates suggest otherwise.

The Army and LSI continue to underestimate the size of software needed for FCS. Studies show this is a common mistake made by defense and private industry that develop software-intensive systems, which can lead to longer schedules and increased cost. Apart from the sheer difficulty of writing and testing such a large volume of complex code, a number of risks face the FCS software development effort. As requirements have become better understood, the number of lines of code has grown significantly since the program began in 2003. Table 1 shows FCS code growth for total source lines of code⁹ (SLOC) and the effective source lines of code¹⁰ (ESLOC).

⁹ SLOC measures the raw size of software.

¹⁰ ESLOC is a surrogate for effort that measures the effective size of reused and adapted code, and is adjusted to its equivalent size in new lines of code. This is not a deliverable product.

Table 1: FCS Software Growth Estimates

Numbers in millions of source lines of code

	Original estimate (May 2003)	Revised estimate (as of January 2006)	Revised estimate (as of August 2007)	Percentage increase
SLOC	33.7	63.8	95.1	182
ESLOC	12.8	17.1	19.6	53

Source: U.S. Army (data); GAO (analysis and presentation).

Since May 2003, projected SLOCs have increased by 61.4 million to an estimated 95.1 million lines of computer software code, almost triple in size compared to original estimates. Similarly, ESLOCs increased by 6.8 million to 19.6 million lines of computer software code, a 53 percent increase. Since January 2006, both SLOC and ESLOC estimates have significantly increased. For example, SLOC estimates increased by 31.3 million lines of computer code, or about 50 percent, while ESLOC estimates increased by 2.5 million lines of computer code, or about 15 percent. Army officials attributed this surge to operating system software that was greatly underestimated in 2003 when the program began. These latest estimates now include operating system software that will be used on the integrated computer system.

While the Army and LSI have completed the first software build—and were close to completing the second of five total software builds at the time of our review—each build required more “actual” software coding than was originally estimated, further indicating that efforts on what it will take to develop and integrate software may be more than planned. For example, the ESLOCs for Build “0” increased 6 percent from an estimated 0.96 million to 1.02 million actual source lines of computer code. Similarly, at the time of our review, ESLOCs for Build “1” increased 17 percent from an estimated 5.3 million lines of code to 6.2 million lines of computer code.¹¹ Army officials maintain that these increases will not have a major impact on the program. However, experiences of other organizations that develop software-intensive systems suggest otherwise, according to leading experts who conducted extensive research of over 20,000 software development projects spanning 18 years. For example, poor size estimation is one of the main reasons that major software-intensive acquisition programs ultimately fail. In fact, the defense industry, private

¹¹ ESLOC data in Build 1 is a cumulative total that includes ESLOCs from Build 0.

sector, and academia note that software size is a critical factor in determining cost, schedule, and effort, and failure to accurately predict software size results in cost overruns and late deliveries. According to guidance made available by the Software Technology Support Center at Hill Air Force Base¹² for defense organizations that develop software, deviations in software size data indicate problems with

- faulty software productivity estimates;
- requirements stability, design, coding, and process;
- unrealistic interpretation of original requirements and resource estimates; and
- rationale used to develop the estimates.

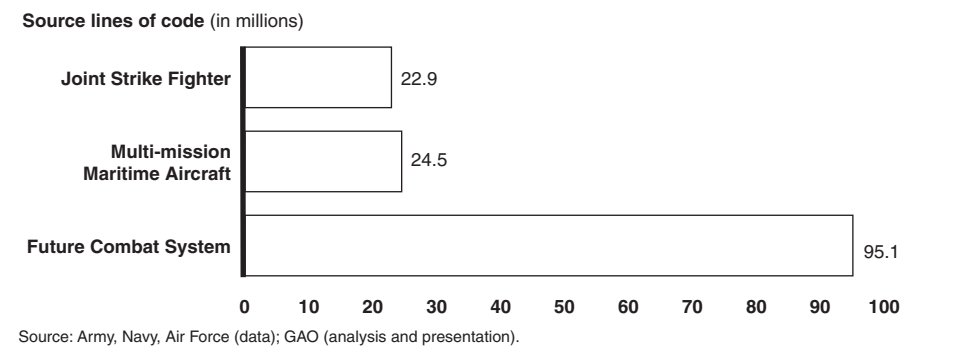
A contributing factor for the Army and LSI's inaccurate software sizing estimates is that system-level requirements have not been fully defined, which makes it difficult to determine what will be needed in terms of software. In May 2003, the Army and LSI estimated that it would take about 34 million lines of code at a time when they were still trying to identify and understand the high-level requirements. Despite not fully understanding those high-level requirements, the Army proceeded with efforts to develop software for FCS. To date, estimating accuracy continues to be hampered by evolving requirements, immature architecture, and insufficient time to thoroughly analyze software subsystems sizing. The difficulties associated with accurate software estimating is an indication that complexity increases as the design is better understood and this serves to increase the level of effort. The potential consequences are longer development time and greater costs.

Taking the latest code estimate into consideration, the total size of FCS's software is about four times larger than the next largest software-intensive defense programs. Figure 4 compares FCS's software SLOC size estimate

¹² In 1987, the U.S. Air Force selected Ogden Air Logistics Center at Hill Air Force Base in Ogden, Utah, to establish and operate its Software Technology Support Center to provide assistance to help organizations identify, evaluate, and adopt software technologies that improve software product quality, production efficiency and predictability. Today, the Center provides services to include, among others, software acquisition best practice support for government organizations, and process maturity appraisals and technology adoption projects across five Air Force major commands, the Navy, the Department of Defense, and the U.S. Treasury Department. The Center also publishes a free journal called *CrossTalk, The Journal of Defense Software Engineering* to more than 24,000 professionals on practical software engineering technologies and best practices.

to the next two largest software intensive defense programs—the Navy’s P-8A Multi-mission Maritime Aircraft, and the Joint Strike Fighter aircraft.

Figure 4: Comparison of FCS Software SLOC Size to Other Major Defense Programs



Independent cost analyses done for FCS have cited software as a likely source of cost growth. According to a June 2006 report issued by the Office of the Secretary of Defense’s Cost Analysis Improvement Group, the FCS program was found to be at risk of higher costs due to, among other things, the size and complexity of the FCS software development program. The Cost Analysis Improvement Group also said that the network is at risk because it is tied to the JTRS and WIN-T programs that could cause delays in FCS’s development schedule. Another study issued in April 2007 by the Institute for Defense Analyses for the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics on FCS costs found that Army plans for developing FCS, including the network, were optimistic with regard to time and money needed for the program. The Institute projected at least \$3 billion in additional FCS development costs due to unplanned software effort including code growth, software integration difficulties, and longer development schedules. The Army does not agree with the Institute’s assessment and believe these issues can be offset.

Software Practices Have Been Adopted, but Implementation Has Been Hampered by Evolving Requirements

The Army and LSI have adopted a number of disciplined software practices, but their effective implementation at the software developer level has been hampered by evolving system-level requirements. In accordance with CMMI¹³ and under the advisory of the Software Engineering Institute, the Army and LSI have adopted software practices that are known to be successful in fostering quality software development, such as disciplined processes, structured management review processes, and an “evolutionary” development process. In our analysis of five FCS software developers, we found that requirements management was the cause of most problems, indicating that a key practice for managing and developing requirements has not been effectively implemented for the five software packages reviewed.

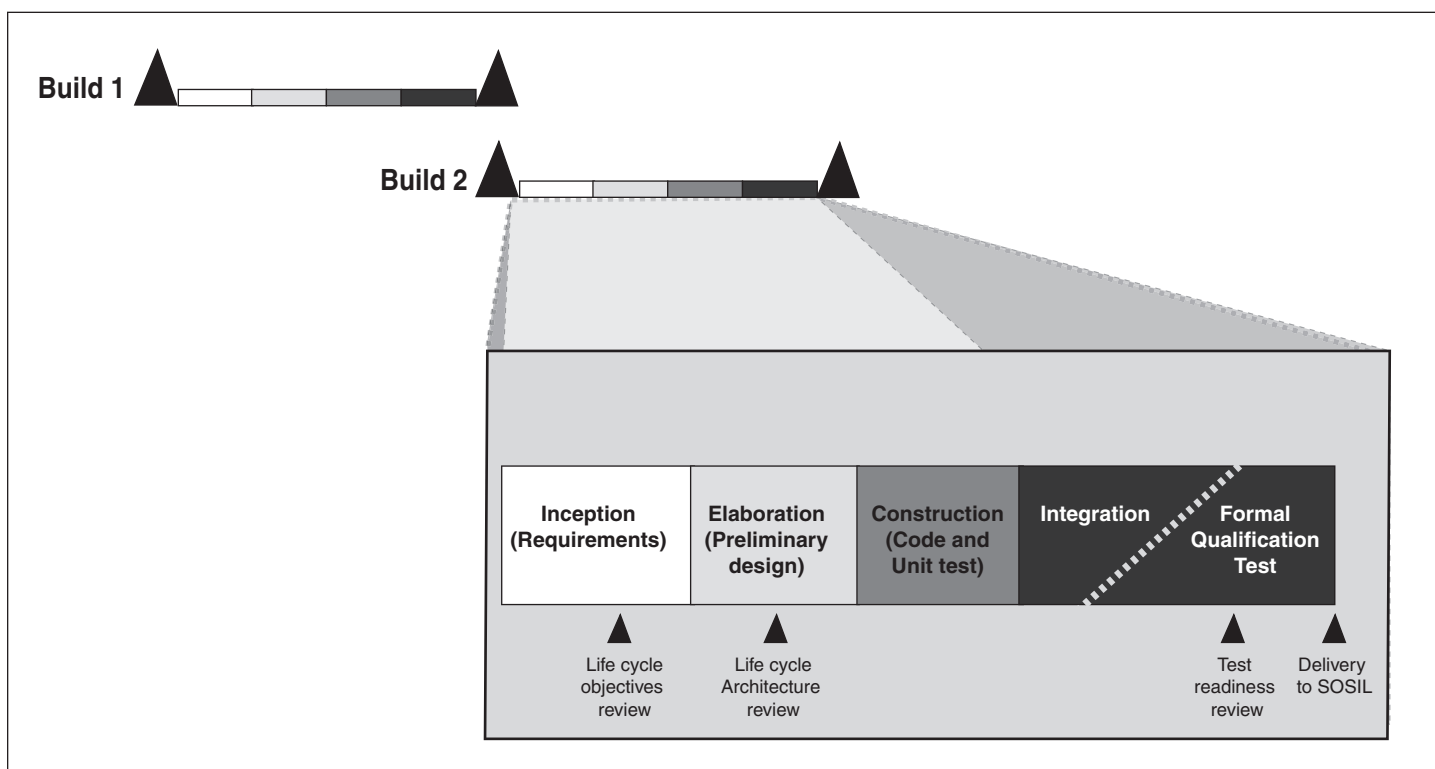
Key Software Development Practices and Processes Used

For FCS software development, the Army and LSI are jointly in charge of oversight and decision-making, and have attempted to do so effectively through the use of disciplined processes, structured management review processes, and an “evolutionary” development process. Seventy-five percent of the FCS software is being developed by 14 software developers (all certified at CMMI level 3 or above) who are developing 52 major software packages. Detailed information about those software developers and what they are responsible for delivering is provided in appendix III.

Through the use of disciplined processes, the Army and LSI have strived to organize and synchronize the large amount of concurrent software development that is taking place. In keeping with the spiral model for development, software development is divided into five builds, and each build has an “early” and “final” stage. Furthermore, each build has four phases—requirements, design, code, and test. Essentially, the spiral model condenses all four phases into builds so that certain interim capabilities can be provided and “spun out” before the entire program is completed. Figure 5 shows a traditional spiral model.

¹³ CMMI[®] (Capability Maturity Model[®] Integration) is a collection of best practices that helps organizations improve their processes. It was initially developed by product teams from industry, government and the Software Engineering Institute for application to process improvement in the development of products and services covering the entire product life cycle from conceptualization through maintenance and disposal. Following the success of CMMI models for development organizations, the need was identified for a CMMI model addressing the acquisition environment.

Figure 5: Traditional Spiral Development Illustration



Source: U.S. Army (data); GAO (analysis and presentation).

The LSI's structured management review processes involve the management of network and software development through the use of several mechanisms that keep track of a series of weekly and monthly program meetings, agendas, progress, and issues. In addition, key metrics are tracked by the software developers and reported to the LSI such as defect age, process compliance, product defects, progress, requirement stability, software development environment, software lines of code, code reuse, and staffing. In the event these metrics reveal a problem or undesirable trend, the LSI takes action to attempt to remedy the situation.

Anchor points are also used by the LSI to maintain structured management review. At a minimum, three software development reviews will be performed for software within a build—life cycle objectives, life cycle architecture, and test readiness reviews. Developers conduct life cycle objective anchor point reviews (or software requirements reviews) to communicate their detailed understanding of the functionality and

performance to be provided by the software item(s) for a given build. Life cycle architecture anchor point reviews (or preliminary design reviews) demonstrate the feasibility of implementing the planned functionality for the software item(s) for a given build within the planned architecture, requirements, cost, and schedule. Successful completion of a formal test readiness review will mean that the developer is ready to start software item formal qualification testing for the applicable software items for a given build.

The Army and LSI also use the evolutionary development process, in which software builds are begun with the understanding that the user need is not fully understood and all requirements cannot be defined up front. In this strategy, user needs and system requirements are partially defined up front and then refined in each succeeding build. The way in which all 52 software packages are being developed at the same time has been called concurrent engineering, which has pros and cons. A pro is that the concurrent development aims to keep the program as a whole on schedule. But software developers reported that when requirements are late or ambiguous, the concurrent engineering approach has a negative cascading effect as all of the software efforts are interrelated.

The Army and LSI are also using modeling and simulation, which takes place in System Integration Labs, and in Huntington Beach, California, at the System of Systems Integration Lab (SoSIL). Since integration and interoperability will be the major challenge in building the FCS, the SoSIL is intended to provide a distributed capability to develop and integrate not only the software but also early hardware and system prototypes to assess and ultimately verify the integration and interoperability of the FCS system of systems and also give program management critical feedback from the user.

Lack of Stable Requirements Has Disrupted Implementation of Good Software Practices

Our analysis of the LSI's software practices and the effect they are having on five subcontracted software developers revealed key problem areas that may be indicators of broader software development problems. We focused mainly on the following areas: Agreement Management, Acquisition Requirements Development, Project Monitoring and Control, Project Planning, and Requirements Management. Of these areas, Requirements Management was found to be the cause of most problems, indicating that a key practice for managing and developing requirements has not been effectively implemented for the five software packages reviewed. In practice, phases within a build are becoming concurrent, and the completion of one build is overlapping the start of the next build.

Software developers stated that additional time, cost, and deferred functionality were the most common results of poorly defined, late, or unstable requirements.

The continuing evolution of FCS system-level requirements, including that caused by Army decisions on what it can afford to develop, and the aggressive pace of the program, are causing disruptions at the software developer level. In an effort to control overall FCS development costs, the Army is reviewing many areas of FCS development, including software, to potentially eliminate areas that are not absolutely essential or critical. Whereas it is a good practice to eliminate these non-essential areas, the drawback is that this causes change in requirements, thereby directly impacting the design and writing of software code. According to LSI officials, changes at the Operational Requirements Document level are not major or frequent, and requirements at that level have actually decreased. Even so, requirements growth and changes are occurring at the system level, which has a cascading effect on the detailed requirements all the way down to the software developer level. The growth results in requirements provided to software developers that are poorly defined, late, or unstable.

For example, developers at iRobot told us they received poorly defined requirements which specified that the small unmanned ground vehicle have a fire extinguisher onboard and be able to withstand direct lightning strikes. Since the small unmanned ground vehicle is a small man-packable robot, these requirements were not practical, but the Army and LSI failed to realize the fundamental differences between this small robot and its other unmanned ground vehicles such as the Multifunction Utility/Logistics Equipment vehicle, which is a 2-1/2 ton vehicle, compared to the small unmanned ground vehicle, which weighs less than 30 pounds. The developer of Battle Command and Mission Execution told us that additional requirements were received after the life cycle architecture review, which is considered late in development. The SOSCOE developers also told us they received late requirements for build 1.8, which caused problems for many other software developers since the late requirements caused them to deliver build 1.8 late and with missing functionality that many developers had expected and were counting on for their own work packages. SOSCOE developers stated that this happened because of misaligned schedules from the top down, and indicated that they too had experienced problems with requirements. Unstable requirements have also been a problem for developers of the Network Management Systems who reported requirements that changed have caused rework in many cases.

Table 2 summarizes problems experienced by the software developers we visited.

Table 2: Software Packages and Associated Requirements Problems

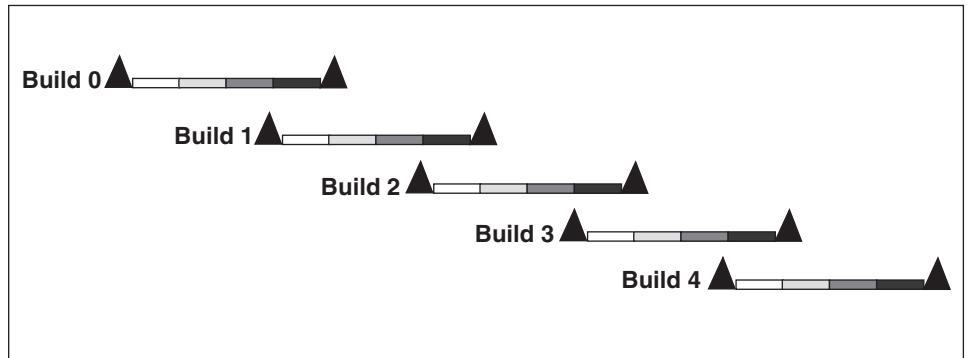
Software packages	Causes			Effect
	Poorly defined requirements	Late requirements	Missing requirements	Deferred functionality
Combat Identification	X		X	
Battle Command and Mission Execution	X	X	X	X
Network Management System	X	X	X	X
Small Unmanned Ground Vehicle	X	X	X	X
Training Common Components	X	X	X	X
System of Systems Common Operating Environment	X	X		X

Source: U.S. Army (data); GAO (analysis and presentation).

Note: SOSCOE is not considered one of the software packages being developed by the 14 first-tier contractors. It is part of the 25 percent of software being developed for FCS by the LSI. We include SOSCOE in this table to point out that problems with requirements effect all levels of software development, from the LSI down to the smallest software package developer.

As shown in table 2, four of the five software developers (and SOSCOE) that we met with report that the problems with requirements have resulted in functionality being deferred to future builds, or waived altogether, for the sake of keeping to the existing schedule. Deferring work into the future means that the associated software code writing and testing will take place later than planned, meaning that more code will be written later and the associated functionality will not be testable until later. These events help partially explain the growth of software estimates already recorded for the early builds. Furthermore, this indicates that less functionality than planned has been delivered and that software estimates will only grow larger in future builds. Overall, software developers told us that these problems could have been avoided if they had been allowed sufficient time to understand and analyze the requirements. This is why the aggressive pace of the program presents such a problem for the development effort. The current FCS practice is to overlap builds more than the traditional spiral model does, as is seen in figure 6.

Figure 6: FCS Spiral Development Strategy and Software Life Cycle Reviews



Source: U.S. Army data; GAO (analysis and presentation).

Before the testing phase is complete on one build, the requirements phase of the next build will start. Program officials told us that the purpose of this is to set requirements so that the next build is ready for design by the time the former build has completed testing. In practice, however, this has been an issue because software developers report that evolving requirements have caused them to interpret and implement changes in requirements well into the design and code phases, compromising the amount of time allotted for testing. This is not to say that the requirements should have been defined more quickly; the state of requirements accurately reflects the maturity of the FCS program. Rather, it is the relative immaturity of the program, coupled with its aggressive pace, that amplify requirements instability, the pronounced overlap of the FCS builds and the cascading effect on software developers.

Uncertainty about Network Development and Demonstration Present Challenges for Decisionmakers at Key Program Events

It is unclear if network requirements, including software to be developed, will be adequately defined and designs completed at the preliminary design review scheduled for February 2009. To date, only some elementary concepts of the FCS network, such as connecting and exchanging information among limited network nodes, have been demonstrated (Experiment 1.1). The first major demonstration of the FCS network is the limited user test scheduled for fiscal year 2012, which will be at least a year after the critical design review and only about a year before the start of FCS low-rate initial production. One of the key objectives of that test will be to identify the contributions and limitations of the network on the ability of the FCS brigade combat team to conduct missions across the full spectrum of operations. The Army hopes that test will be enough to meet the congressional requirement to conduct a network demonstration prior

to obligating any funds for FCS low-rate initial production of manned vehicles.

Unclear Picture of Network Status and Outlook at 2009 Milestone Review

A substantial amount of development work remains before the Army and LSI can demonstrate the full expected capability of the network. Modeling and simulation are being employed as key parts of the FCS network and software development process. While modeling and simulation is a cost effective approach for proving out technological advances incrementally, this approach has limitations in predicting the performance of first-of-kind systems. For example, commercial firms in the past have learned that modeling and simulation is very reliable for predicting the performance of products that are evolutionary advances over existing products, for which there is a large base of experience to draw from. However, it is generally understood that without sufficient data on past behavior and a better understanding of assumptions, the results of modeling and simulation may not entirely reflect the workings of the new or advanced systems. A number of limited demonstrations have been scheduled within the FCS system development and demonstration phase to help move the Army toward a network-centric environment. To date, only basic network concepts, such as connecting and exchanging information among limited network nodes have been demonstrated (Experiment 1.1). The Army plans to demonstrate some network functions, such as linkage with remote sensors, during the spinout demonstration in 2008. Other demonstrations are scheduled in 2010 and 2012. However, the fully automated battle command system is not expected until 2013 when the Army envisions 100 percent of network capabilities such as the full networked joint and multi-national battle command, full interoperability and network integration with platforms, full sensing and targeting, full networked logistics, and planning and training services. This event will occur near the time of the FCS production decision, after the designs on manned ground vehicles have been established.

At the time of the FCS milestone review in 2009, the extent of network demonstration is expected to be very limited. For example, the Army plans to demonstrate, among other basic things, sensor control, terrain analysis, and unmanned platform planning and operations in 2008. As mentioned earlier, network design and maturity are in the early stages as the Army and LSI are still determining what network management means in terms of what is needed to support each specific mission, how to allocate network resources to the mission spectrum, how to fuse, process, and present extensive FCS sensor data to appropriate users, and how to maintain the network. The Army is still in the midst of stabilizing the network and

software requirements, and hardware and software designs are still maturing. Further, there is uncertainty about when the network requirements will be fully defined. More importantly, it is unclear, if not doubtful, that recognized technical risks will be reduced to acceptably low levels by the 2009 review.

Major Demonstration of FCS Network Scheduled in 2012 after Vehicle Designs Are Set

The first major demonstration of the FCS network is limited user test 3 scheduled for fiscal year 2012, which will be at least a year after critical design review and about a year before the start of low-rate initial production for the core FCS program scheduled to begin in 2013. By then, billions will have been spent and it may be too late to fix any network problems revealed in this significant test before production begins. At critical design review in 2011, the Army expects that the FCS network capabilities will be completed on the manned platform planning and operations. In section 211 of the recently enacted National Defense Authorization Act for Fiscal Year 2008, Congress directed that a network demonstration be conducted prior to obligation of funds for low-rate initial production (Milestone C) or full-rate production of FCS manned ground vehicles.¹⁴ One of the key objectives of that test will be to use FCS prototypes to identify the contributions and limitations of the network on the ability of the FCS brigade combat team to conduct missions across the full spectrum of operations. The limited user test 3 will be pivotal to the FCS program because it is the first test event to incorporate each of the 14 FCS platforms, and it serves as a seminal event to generate system-of-systems test data to underpin the modeling and simulation environment used to support the test. However, the fully automated battle command system is not expected until 2013 when all the software application capabilities are expected, including the full networked joint and multinational battle command, interoperability, integration of all platforms, integrated training, sensing and targeting, and other functions.

Even if the demonstration of the network takes place in 2012 as planned, it will follow the design reviews of the other FCS systems. The design of these systems depends significantly on the performance of the network, such as its delivered quality of service. There are a number of FCS systems or platforms, such as manned ground vehicles,¹⁵ that are scheduled to have

¹⁴ Pub. L. No. 110-181, § 211 (2008).

¹⁵ FCS manned ground vehicles includes infantry carrier vehicles, non-line of sight cannon, mounted combat system, reconnaissance and surveillance vehicles, command and control vehicles, non-line of sight mortar, and support vehicles.

their critical design reviews in fiscal years 2009-2010, about 2 years before the first major demonstration of the network in fiscal year 2012. For manned ground vehicles, most developmental prototypes will be in testing and the Army will have begun preparation for low-rate initial production for these platforms before the network is demonstrated. This is a significant risk as the software, which supports the information network, is critical to the design and performance of the platforms and is expected to control about 95 percent of FCS's functionality. If the network underperforms, it could affect the lethality and survivability of the vehicles. Because of this sequence of events, there will be little opportunity for the vehicle designs to compensate for any shortfalls in network performance.

Conclusions

The advanced information network is the linchpin to the Army's FCS concept; yet, it is unclear whether, how, or when the Army will be able to demonstrate that the network performs as needed. The Army and the LSI have focused a great amount of attention on the network and software, evidenced by the sound development practices they have attempted to put in place. However, network and software requirements are not yet stable at the system level and below, which has caused rework and deferred functionality. Such instability may be expected given the relative immaturity of FCS, but the program is halfway through development and the remaining schedule is very ambitious; program decisions have been and will continue to be made in advance of acquisition knowledge. Demonstrations to date have been small and not sufficient—nor intended—to prove the network's performance. Large-scale demonstrations of the network's ability to deliver the quality of service essential to the FCS fighting concept will not come until 2012, the year before the low-rate initial production decision, assuming the remainder of development goes as planned. Even if this date is met, it will trail the critical design reviews of the individual FCS systems by 2 years. This is disquieting because the designs of the systems—including the manned ground vehicles—depend on the quality of service delivered by the network. Finally, the overall magnitude of the FCS software effort has nearly tripled to 95 million lines of code. This growth gives credence to the higher cost estimates put forth by the Cost Analysis Improvement Group and the Institute for Defense Analysis—both of which concluded that the FCS software effort would be more extensive than the Army envisioned.

For these reasons, it is essential that the software and network efforts be held to meeting clear performance criteria at key junctures that are linked to the network's needed quality of service. These junctures include the

2009 milestone review, the 2009-2010 vehicle critical design reviews, the 2011 FCS critical design review, and the 2012 network demonstration. Allowing demonstrations or network functions to be deferred past these junctures on the basis that modeling and simulation results are promising will not suffice. Given the difficulty of predicting performance in full-scale operations, testing must be the primary basis for judging the sufficiency of progress. Because the performance of the network and the success of the software effort are not assured, decision makers should allow for the possibility that full success will not be achieved. Thus, it will be wise to keep alternative courses of action viable to guard against such an eventuality.

Recommendations for Executive Action

We recommend that the Secretary of Defense:

- Direct the FCS program to stabilize network and software requirements on each software build to enable software developers to follow disciplined software practices, including having realistic and synchronized test schedules.
- Establish a clear set of criteria for acceptable network performance at each of the key program events including the
 - 2009 milestone review,
 - platform and system-of-system critical design reviews,
 - major network demonstration in 2012, and
 - Milestone C for core FCS program.

We further recommend that the Secretary of Defense, in setting expectations for the 2009 milestone review, include

- a thorough analysis of network technical feasibility and risks,
- synchronization of network development and demonstration with that of other elements of FCS such as the manned ground vehicles, and
- a reconciliation of the differences between independent and Army estimates of network and software development scope and cost.

Agency Comments and Our Evaluation

DOD concurred with our recommendations and stated that growing the networking capability of the ground forces is a priority and network development for FCS is a critical element in the Army's effort to modernize its tactical network. In recognizing FCS's network development and importance to the Army's efforts to modernize the tactical network, DOD stated that criteria for network performance would be established.

The criteria for network performance would be documented in the FCS acquisition strategy, the system engineering plan, and test plans. However, because these documents will not be updated until the 2009 milestone review, that could leave in question what will be expected in terms of network performance by the time of the 2009 milestone review itself. DOD should establish in advance the network criteria that will be applied at the 2009 milestone review, such as at the time of the annual review to be held in 2008.

In concurring with our recommendation on setting expectations for the 2009 milestone review, DOD stated that an analysis of network technical feasibility and risks will inform the FCS 2009 review. DOD further stated that manned ground vehicle and network development and demonstration will be synchronized and that the 2009 FCS review will evaluate the network and software cost estimates and cost risks identified for the development, integration, and testing of the FCS network and software. These are constructive steps that will contribute to the FCS milestone review in 2009. However, we believe that DOD needs to go beyond evaluating cost estimates and risks. The differences between the Army's estimate and independent cost estimates have been substantial. The lower Army estimate has been allowed to prevail, without a determination that it is the better estimate—that is, the one more likely to accurately predict the actual cost of FCS. DOD, in determining the official cost estimate for FCS, should provide the rationale for its position. Heretofore, the Army's estimates have been constrained by available funding and Army officials have stated that they will reduce program scope if costs are higher than expected. If FCS is found to be worth doing in its entirety during the 2009 milestone review, its most likely cost should be understood.

We also received technical comments from DOD which have been addressed in the report, as appropriate.

We are sending copies of this report to the Secretary of Defense; the Secretary of the Army; and the Director, Office of Management and Budget. Copies will also be made available to others on request. In addition, the report will be made available at no charge on the GAO Web site at <http://www.gao.gov>.

If you, or your staff, have any questions concerning this report, please contact me at (202) 512-4841. Contact points for our offices of Congressional Relations and Public Affairs may be found on the last page of this report. The major contributors are listed in appendix IV.

A handwritten signature in black ink that reads "Paul L. Francis". The signature is written in a cursive style with a large, stylized 'P' and 'F'.

Paul L. Francis
Director
Acquisition and Sourcing Management

List of Congressional Committees

The Honorable Carl Levin
Chairman
The Honorable John McCain
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Daniel K. Inouye
Chairman
The Honorable Ted Stevens
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

The Honorable Ike Skelton
Chairman
The Honorable Duncan L. Hunter
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable John P. Murtha
Chairman
The Honorable C. W. (Bill) Young
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

Appendix I: Scope and Methodology

To develop the information on the Future Combat System program's network and software challenges and technological risks, assess whether disciplined software practices have been effectively implemented, and determine whether the Army will have the necessary network and software at key program events, we interviewed the Assistant Secretary of the Army (Acquisition, Technology, and Logistics); the Program Manager for the Future Combat System (Brigade Combat Team); the Future Combat System Lead Systems Integrator; officials from the Army's Software Engineering Directorate; and Lead Systems Integrator One Team contractors. We selected 5 of 52 software packages and conducted detailed structured interviews to determine how the use of the LSI's software best practices affected the developers at various levels within FCS. In consultation with the Army, LSI, University of Maryland (Fraunhofer Center for Experimental Software Engineering) and experts from GAO's Applied Research and Methods group, we selected software packages that are critical to FCS's network and those that would provide a good cross section of the development efforts being conducted by contractors under LSI's direction. This software included the Battle Command and Mission Execution, Combat Identification, Network Management System, Small Unmanned Ground Vehicle, and Training Common Components. Limited work was conducted on SOSCOE. We reviewed, among other documents, the Future Combat System's Integrated Master Schedule and CMMI Evolution, Test and Evaluation Master Plan, Software Configuration Management, Development, Integration, Quality Assurance, Risk Mitigation, and Measurement Plans. In addition to CMMI for Acquisition, Version 1.2, we also reviewed individual software developers' Software Development, Configuration Management, Integration, Quality Assurance, System Engineering Management, Risk and Opportunity Management, and Test Plans, Software Architecture Description Documents, and Software Requirements Specifications. We attended FCS Board of Director's meetings and the Delta Engineering Iteration 2 Definition Anchor Point and System of Systems Build 2 Definition Checkpoint Review. In our assessment of the FCS network and software development, we used the knowledge-based acquisition practices drawn from our large body of past work as well as DOD's acquisition policy and the experiences of other programs. We discussed the issues presented in this report with officials from the Army and the Secretary of Defense and made changes as appropriate. We performed our review from July 2007 to March 2008 in accordance with generally accepted auditing standards.

Appendix II: Comments from the Department of Defense



OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

FEB 28 2008

ACQUISITION,
TECHNOLOGY
AND LOGISTICS

Mr. Paul L. Francis
Director, Acquisition and Sourcing Management
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

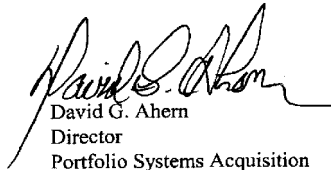
Dear Mr. Francis:

This is the Department of Defense (DoD) response to the GAO draft report, "DEFENSE ACQUISITIONS: Significant Challenges Ahead in Developing and Demonstrating Future Combat System's Network and Software," dated January 31, 2008 (GAO Code 120667/GAO-08-409).

The report recommends that the Secretary of Defense direct the Future Combat System (FCS) program to stabilize network and software requirements on each software build and establish criteria on acceptable network performance for each key program event.

The Department concurs with the GAO recommendations and our comments are enclosed. Growing the networking capability of the ground forces is a Department priority and the FCS network development is a critical element in the Army's effort to modernize its tactical network. Acquisition of networking capability requires a disciplined, yet agile, acquisition construct. The network aspect of the FCS program is an important component of the periodic acquisition reviews of FCS conducted by the Department, including the Defense Acquisition Board review subsequent to the FCS preliminary design review in 2009. Detailed technical comments were provided separately.

Sincerely,


David G. Ahern
Director
Portfolio Systems Acquisition

Enclosure:
As stated



GAO DRAFT REPORT DATED JANUARY 31, 2008
GAO-08-409 (GAO CODE 120667)

**“DEFENSE ACQUISITIONS: SIGNIFICANT CHALLENGES AHEAD IN
DEVELOPING AND DEMONSTRATING FUTURE COMBAT SYSTEM’S
NETWORK AND SOFTWARE”**

**DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATION**

RECOMMENDATION 1: The GAO recommended that the Secretary of Defense direct the Future Combat System (FCS) program to stabilize network and software requirements on each software build to enable software developers to follow disciplined software practices, including having realistic and synchronized test schedules.

DOD RESPONSE: Concur. The FCS program will finalize and release network and software requirements prior to each software build. The test schedules for each build, and for overall system network testing, will be documented and synchronized for realistic, informed network assessments.

RECOMMENDATION 2: The GAO recommended that the Secretary of Defense, establish a clear set of criteria for acceptable network performance at each of the key program events including the following:

- a. 2009 milestone review;
- b. platform and system-of-system critical design reviews;
- c. major network demonstration in 2012, and;
- d. milestone C for core FCS program.

DOD RESPONSE: Concur. Criteria for network performance for key program events shall be established. These criteria shall be reflected in the appropriate program documentation. The update to the FCS Acquisition Strategy shall include network performance criteria for the 2009 Defense Acquisition Board and Milestone C. The update to the FCS System Engineering Plan shall reflect network performance criteria anticipated for the platform and system-of-system critical design reviews. The assessment criteria for network performance shall be documented in test plans for test events to include the Technical Field Tests and Limited User Tests.

RECOMMENDATION 3: The GAO recommended that the Secretary of Defense, in setting expectations for the 2009 milestone review, include:

- a. a thorough analysis of network technical feasibility and risks;
- b. synchronization of network development and demonstration with that of other elements of FCS such as the manned ground vehicles, and;
- c. a reconciliation of the differences between independent and Army estimates of network and software development scope and cost.

DOD RESPONSE: Concur: An analysis of network technical feasibility and risks will inform the FCS 2009 review. Additionally, manned ground vehicle and network development and demonstration will be synchronized in the areas where there are interfaces and dependencies. The 2009 FCS review will evaluate the network and software cost estimates and cost risks identified for the development, integration, and testing of the FCS network and software.

Appendix III: List of FCS Software (Network & Non-network) Packages Developed by Contractors (as of July 2007)

FCS contractors (First-tier)	Number of software packages	Name of software (network and non-network) packages
AcuSoft, Inc.	1	Training Common Components Software Suite ^a
AT&T GSI	1	Training Common Components Software Suite ^a
BAE Systems	10	Acoustic Locating Array Subsystem; Emitter Mapper Subsystem; Ground/Air Platform Communication; FCS Recovery and Maintenance Vehicle operational; Infantry Carrier Vehicle operational; Medical Vehicle operational; Common operational (all 8 manned ground vehicles); Non Line of Sight Cannon operational; Non Line of Sight Mortar operational; Armed Robotic Vehicle
DRS	3	Short-range Electro-optical sensor; Small Unmanned Ground Vehicle Electro-optical Infrared; Class 1 Electro-optical Infrared
General Dynamics	8	Autonomous Navigation System ^a ; Sensor Data Management ^a ; Planning/Preparation Services ^a ; Integrated Computer Services; Command and control vehicle operational; Mounted combat system operational; Reconnaissance and surveillance vehicle operational; Common operational (all 8 manned ground vehicles)
Honeywell	5	Vehicle Management Computer; Board Support Package (for Vehicle Management Computer, Psuedo-integrated Computer System, & vehicle simulation); Platform Soldier Readiness System ^a
IBM	3	Logistics Data Agent ^a ; Logical Data Manager ^a ; Logistics Data Management Service ^a
iRobot	2	Small Unmanned Ground Vehicle operational and Small Unmanned Ground Vehicle modeling and simulation
Lockheed Martin	5	Warfighter Centralized Controller Device ^a ; Common Electro-Optical Sensor; Level 1 Fusion ^a ; Training Common Components Software Suite ^a ; Vehicle Control, Mobility control, weapons control, power service, vehicle management
Northrop Grumman	5	Class IV Unmanned Aerial Vehicle; Logistics Decision Support System-Manned Ground Vehicle ^a ; Air Sensor Integration ^a ; Aided Target Recognition; Network Management ^a
Overwatch Systems	1	Situation Understanding ^a
Raytheon	5	Ground Sensor Integrator ^a ; Combat Identification ^a ; Multi-function radio frequency; Common Electro-Optical Sensor; Battle Command and Mission Execution ^a
SAIC	1	Training Common Components Software Suite ^a
Textron	2	Tactical and Urban Ground Sensors; Unattended Ground Sensors
Total: 14	Total: 52	

Source: U.S. Army (data); GAO (analysis and presentation).

^a Software packages expected to provide partial or full networking functions.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Paul L. Francis (202) 512-4841 or FrancisP@gao.gov

Acknowledgments

In addition to the individual named above, William R. Graveline, Assistant Director; John M. Ortiz Jr.; Letisha T. Watson; Helena Brink; Noah B. Bleicher; Robert S. Swierczek; and Senior Technologists Madhav S. Panwar and Dr. Hai V. Tran made key contributions to this report.

Related GAO Products

Defense Acquisitions: Role of Lead Systems Integrator on Future Combat Systems Program Poses Oversight Challenges. [GAO-07-380](#). Washington, D.C.: June 6, 2007.

Defense Acquisitions: Future Combat System Risks Underscore the Importance of Oversight. [GAO-07-672T](#). Washington, D.C.: March 27, 2007.

Defense Acquisitions: Key Decisions to Be Made on Future Combat System. [GAO-07-376](#). Washington, D.C.: March 15, 2007.

Defense Acquisitions: The Army Faces Challenges in Developing a Tactical Networking Strategy. [GAO-07-10SU](#). Washington, D.C.: October 4, 2006.

Defense Acquisitions: Restructured JTRS Program Reduces Risk, but Significant Challenges Remain. [GAO-06-955](#). Washington, D.C.: September 11, 2006.

Defense Acquisitions: Improved Business Case Key for Future Combat System's Success. [GAO-06-564T](#). Washington, D.C.: April 4, 2006.

Defense Acquisitions: Assessments of Selected Weapon Programs. [GAO-07-406SP](#). Washington, D.C.: March 30, 2007.

Defense Acquisitions: Improved Business Case is Needed for Future Combat System's Successful Outcome. [GAO-06-367](#). Washington, D.C.: March 14, 2006.

Defense Acquisitions: Business Case and Business Arrangements Key for Future Combat System's Success. [GAO-06-478T](#). Washington, D.C.: March 1, 2006.

Defense Acquisitions: Resolving Development Risks in the Army's Networked Communications Capabilities is Key to Fielding Future Force. [GAO-05-669](#). Washington, D.C.: June 15, 2005.

Defense Acquisitions: Future Combat Systems Challenges and Prospects for Success. [GAO-05-428T](#). Washington, D.C.: March 16, 2005.

Defense Acquisitions: Future Combat Systems Challenges and Prospects for Success. [GAO-05-442T](#). Washington, D.C.: March 16, 2005.

Defense Acquisitions: The Global Information Grid and Challenges Facing Its Implementation. [GAO-04-858](#). Washington, D.C.: July 28, 2004.

Defense Acquisitions: The Army's Future Combat Systems' Features, Risks, and Alternatives. [GAO-04-635T](#). Washington, D.C.: April 1, 2004.

Defense Acquisitions: Stronger Management Practices Are Needed to Improve DOD's Software-Intensive Weapon Acquisitions. [GAO-04-393](#). Washington, D.C.: March 1, 2004.

Issues Facing the Army's Future Combat Systems Program. [GAO-03-1010R](#). Washington, D.C.: August 13, 2003.

Defense Acquisitions: Army Transformation Faces Weapon Systems Challenges. [GAO-01-311](#). Washington, D.C.: May 2001.

Best Practices: Better Matching of Needs and Resources Will Lead to Better Weapon System Outcomes. [GAO-01-288](#). Washington, D.C.: March 8, 2001.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548